TECHNICAL ARCHITECTURE REVIEW

Project Name:	**Authentication, Authorization, and Single Sign On (SSO) Technologies**
Requestor:	Ken Peterson and Darcie Trimble
Date of Initial Request:	October/December 2007
Request Description:	Prepare a review of technology options and best practices for SSO and related authentication, authorization, and identity management services.
Agency or Agencies:	DTS (Enterprise Service Infrastructure)
Reviewers:	Bob Woolley, Darrus McBride and Dave Fletcher
ARB Acceptance Date:	
Agency Requestor Acceptance Date:	

Objectives and Scope of Review

The Utah Master Directory (UMD) and related SiteMinder architecture was designed in 2001. There is a need to validate current practices against best practice industry solutions with an objective of wider adoption of the Single Sign-On (SSO) and related directory and access control infrastructure. This report will provide a comprehensive review of alternative technologies and a baseline of current UMD/SiteMinder adoption within State government.

Introduction

The term SSO is replete with multiple meanings and definitions. For purposes of this review the following definitions have been applied:

- **Enterprise SSO**—The primary user community consists of employees. Application types that are supported typically include desktop client and browser based applications. The architecture and implementation often supports a protected password vault and may include credential based form fills.

- **Web SSO**—The user communities include employees, business partners, and customers. Application types are generally browser based. The architecture and implementation supports: HTTP session management;

application security shims; Role Based Access Control (RBAC); single security domain; and, user accounts.

- **Federated SSO**—The user communities include employees, business partners, and customers. Application types are generally browser based and include Web services. The architecture and implementation supports: identity assertions; role and attribute exchange; and, spanning of security domains. User accounts may not be required.

- **Web and Personal SSO**—This is a user managed domain that utilizes Internet resources.

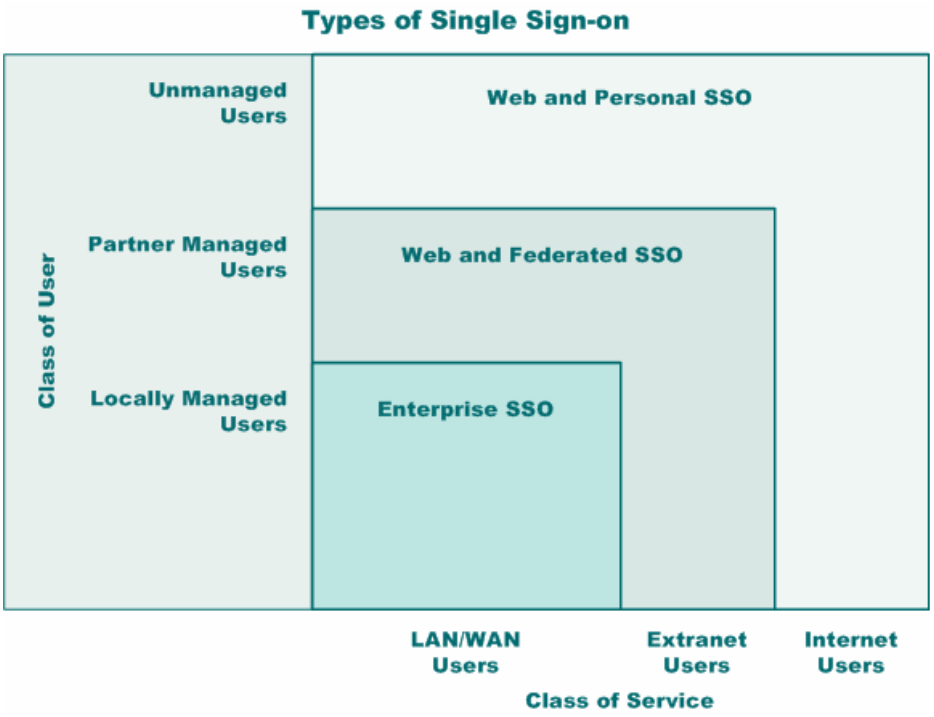

Figure 1. Types of Single Sign-On

SSO is a component of an Identity Access Management (IAM) ecosystem. The IAM ecosystem combines several types of technology components that are illustrated in Figure 2 (adapted from a drawing by Forrester[1]). This drawing illustrates the current roles of existing UMD Services, and, in the case of the audit function, highlights an area where tool sets need to be better defined.

[1] Cser, Andras and Penn, Jonathan, *Identity Management Market Forecast: 2007 To 2014*, Forrester Research, February 2008, p. 3.

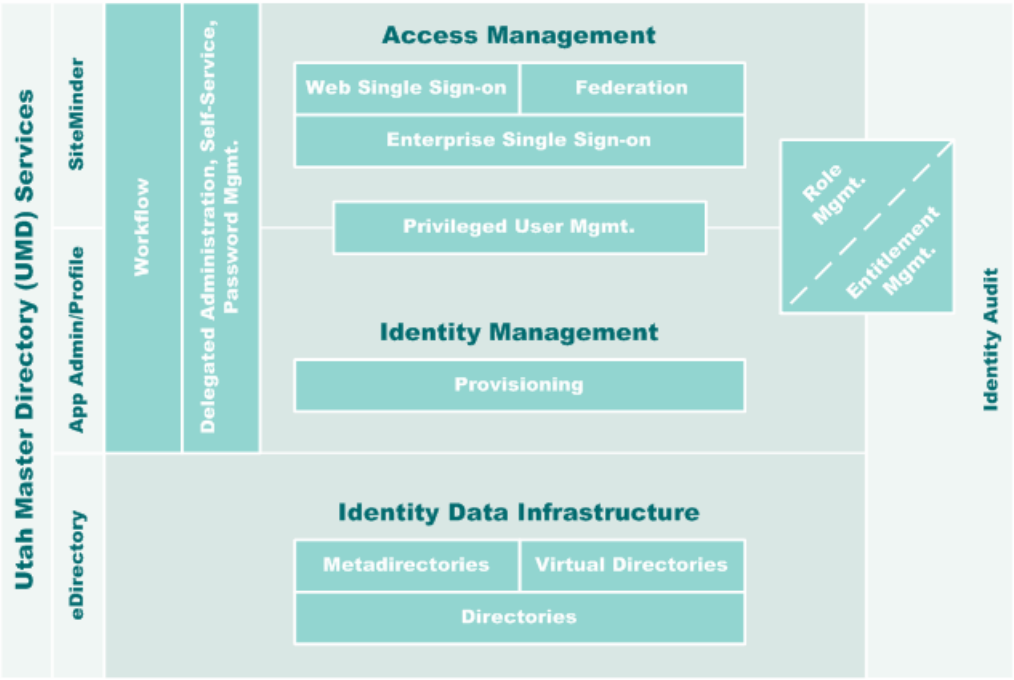

Figure 2. Identity Access Management Ecosystem

- **Identity Data Infrastructure**—This component includes products that form the identity information layer, including directories, meta directories, and virtual directories. This layer is represented within the State by Novell's eDirectory and other associated directory infrastructure components.

- **Identity Administration: Accounts and Privileges Administration**—Products that manage users' accounts, attributes, and credentials include provisioning and role, password, and privileged user management. This category also includes the functional elements of self-service and delegated administration. This component is represented by Application Profile within the State, and other potential resources, such as RACF, in the mainframe environment.

- **Access Management: Access Control to IT Resources**—Coordinating user access to multiple applications is the domain of products like enterprise single sign-on (E-SSO), Web single sign-on (Web SSO), and federation. It also includes the emerging area of entitlement management. The Utah Master Directory (UMD) services control access rights to a wide range of applications. Access control for Web applications is supported by the CA SiteMinder product on an enterprise level.

- **Identity Audit: Administrative and Access Activities**—The State requires the ability to demonstrate that account administration and access controls are performing according to policy. Identity audit products help

with this effort. This includes auditing tools that combine and correlate activities and events across the identity infrastructure, as well as privilege attestation tools to aid the act of certifying that the privileges associated with a user are correct. It also includes role management products, which serve a dual role of both codifying policies and validating their enforcement. This is an area that needs more development within the State. Currently most auditing functions are handled at the application level, if at all.

Baseline of Current Architecture

The Utah Master Directory (UMD) is an identity management system for all State of Utah employees and approved citizens. It is designed to be the touchstone for all applications requiring authentication and authorization, providing a single, up to date database of consistent user information as well as a single sign on solution when a user ID and password are required for access.

Prior to UMD, the State of Utah had many authorized user directories; one for almost every online application. The application administrator had to create dedicated accounts for the users, and the users had to remember an ID and password for each secure application they accessed. In addition, application administrators were not consistently notified when there was a change in an employee's status. A single enterprise authentication directory seemed to be the answer; one that used the Human Resource database as its "source of truth," providing the most accurate and up to date user profile available. An application was designed, programmed, and tested. The completed Utah Master Directory was placed into production in July 2002.

UMD has proven to be a fast, accurate employee provisioning and de-provisioning solution. Now, each State employee has only one user ID and password to remember, allowing access to all participating State applications. And now, when an employee terminates State employment, accounts with all associated systems are automatically disabled. Associated systems allow enterprise collaboration and improve reliability and security. Just a few of these applications include a white pages application to view employee information (including organization charts, phone numbers, and work addresses); instant messaging applications; and, employee time sheets.

Core UMD Services components include:

- **UMD Directory**—UMD is a directory of multiple sets of users, including employees, some local government entities, and citizens. Human Resources controls all employee records within UMD, making additions, deletions, and modifications which are reflected within the UMD data. Public accounts are created and maintained by the users in a Credential Collector Web form. UMD also provides data to the LAN directory for automatic provisioning of user accounts, and any modifications to the LAN

accounts are synchronized with UMD. Access to the UMD is through the LDAP protocol, and UMD data is strictly controlled.

- **SiteMinder**—SiteMinder, from CA, provides highly secure authentication and authorization of Web resources. An encrypted browser cookie maintains the SiteMinder session. The session cookie is sent to all "utah.gov" domains that a browser visits. Through this method, SiteMinder provides an SSO environment where users are authenticated against the UMD directory. Currently ID and password authentication schemas are supported. The password is stored in the directory as a public or private key pair and is not retrievable. SiteMinder authorizes every URL in the protected realm. Authorization or access is allowed based on information in the user's UMD account.

- **Credential Collector**—The credential collector is a J2EE Web application created by DTS. Its functions include:

    - Provision of a standard SiteMinder system login ID, which is the directory Domain Name (DN).
    - Provision of a standard password restoration method for forgotten passwords for both public and employee users.
    - Provision of a means to create public user accounts.
    - Provision for e-mail address verification for creating "trust" in the account.
    - Provision of account maintenance functions for both public and employee accounts.

  Users may use an alias, an e-mail address, or their employee ID# to log in. The alias can be set to anything the user desires, and may be changed by the user, as long as the value remains unique. The e-mail address can be changed by public users and will trigger an address verification process.

- **AppProfile System**—The application profile system is a client/server system written in Java. The purpose of the system is to provide very flexible and secure access to the UMD. AppProfile is similar to a database. Multiple AppProfile servers provide the database functionality, while the AppProfile Client provides the database client function. Features include:

    - the ability to extend the UMD schema for the addition of custom attributes;
    - field types, including Binary, Selection, Option, Text, Existing-Text, Encrypted-Text, Date, and Number;
    - agency access control;

  - controlled access based upon a “scope” to limit the view of accounts;
  - group attributes under the control of different profiles into “types.”
  - values given to groups of user accounts based on a priority level;
  - the ability to search for accounts having certain attribute values in a profile;
  - the ability to search the general directory of accounts within a scope; and,
  - a caching system for storing retrieved data for quick reference.

- **AppAdmin**—This is a J2EE Web application that provides a general-purpose implementation of the AppProfile client. All the functions performed by AppAdmin are available to programmers using the AppProfile client directly. By using AppAdmin, programmers will not need to learn the complexities of schema administration, and AppAdmin may fulfill the requirements of the application administration and thus eliminate the need to create a custom administration piece in their application.

- **JAAS Providers to Application Servers**—Java Authentication and Authorization Servers (JAAS) is a standard API that application developers can use when creating an application. While developing the application, the developer may use a file based JAAS provider, then, when ready to deploy to a SiteMinder/UMD protected server, the JAAS roles are just mapped to roles stored in UMD, and easily passed with SiteMinder. Providers have been created for WebSphere, SUN AppServer 7, GlassFish, and Tomcat. The providers use information from the AppProfile system to provide role membership information into JAAS.

These architecture components constitute an IAM environment for the State that leverages commercial products and custom Java applications.

User Adoption Data

A survey (see Appendix A for detailed responses) was conducted with IT directors using a Web-based survey instrument that gathered information on UMD utilization, adoption, and obstacles to use. Conclusions that could be drawn from the survey include:

- Overall integration with existing applications inventory is less than 30%.

- Application specific directory and authorization is used by 65.4% of all production applications.

- Direct LDAP to agency directory information is utilized by 23.1% of production applications.

- Existing UMD/SiteMinder users reported the following as successful features of the UMD environment:

    - Integration with NDS to Synchronize LAN Passwords: 50.0%
    - Availability of UMD/SiteMinder Infrastructure: 40.9%
    - Identity Management: 22.7%
    - Simplified Maintenance of User Access Privileges: 18.2%
    - UMD Support Services: 18.2%
    - Reliability and Scalability: 4.5%

- Over 40% of survey respondents reported that they did not use the UMD.

- Obstacles that kept agencies from using UMD Services included:

    - Difficulty Using the UMD with New Applications: 22.7%
    - Difficulty Using the UMD with Existing Applications: 22.7%
    - Direct LDAP Access: 18.2%
    - Reliability and Scalability Concerns: 18.2%
    - Inadequate Documentation: 13.6%
    - Cost Concerns: 13.6%
    - Availability of UMD Web Services: 13.6%
    - Application Profile Management: 9.1%
    - SSO Security Concerns: 9.1%
    - Concerns with the Use of "Cookies": 4.5%

- Only 36.4% of all respondents perceived a high priority need for SSO within the enterprise.

- Only 31.8% of all respondents perceived a high importance for strong authentication.

If nothing else, the survey demonstrates a substantial need for IAM training across the enterprise. One of the more telling respondent comments regarding SSO was that they "…did not need it, they authenticated within the application." This is a rather substantial gap between behavior and best practices.

Help Desk Data

One of the initial goals and business drivers for the UMD was to reduce the cost of password resets and related directory and network access issues. Approximately one out of three Help Desk calls involve password reset.[2] IT Security Journal[3] estimates that 30% of all help desk calls involve password problems.

[2] Phifer, Lisa, "Identity management appliances reduce password cost." Core Competence, July 21, 2006.
[3] Cicchitto, Nelson, *Evaluating Your Identity and Access Management Options*, IT Security Journal, October 1, 2007.

Significantly, the existing UMD Services environment has reduced reset calls to less than 3% of total Help Desk calls. This is 1/10th of what might be expected. If Network/LAN and UMD calls are combined, the total is less than 6%, or 1/5th, of what might be assumed. All password resets account for only about 9%. Help Desk data illustrated in Table 1 is indicative of the current call data for software resets in the current UMD, Network/LAN, and Mainframe environments.

Table 1. Help Desk Call Data for Password Resets and UMD Related Inquiries.

	1st Q '07	2nd Q '07	3rd Q '07	4th Q '07	Jan '08	Feb '08
Network/LAN PW Reset	485	587	693	740	251	245
Mainframe PW Reset	385	380	421	382	147	101
UMD PW Reset	484	618	594	624	264	242
Total	1354	1585	1708	1746	662	588
Total Tickets	17,812	18,240	19,342	19,089	7,604	6,813
% PW Resets	7.6%	8.7%	8.8%	9.1%	8.7%	8.6%

This data is impressive for the applications and Network/LAN logins that are associated with the UMD. It is useful to remember that 75% of all other application password maintenance is being handled within agencies. These requests are largely not reflected in Help Desk data. This represents a substantial additional cost burden for agency IT personnel that could be improved with greater UMD Services adoption.

Best Practices Review

Top single sign-on considerations for SSO solutions are a critical part of a State IT infrastructure and the way employees do business and interact with needed information. Increasingly, SSO is being viewed as a component of a comprehensive IAM product group. A number of authors have identified the following as key issues to keep in mind while evaluating SSO solution alternatives:

1. **Application Coverage**—Optimize the number of applications that utilize IAM/SSO services and infrastructure.

2. **Ease and Flexibility of Deployment**—Deployment complexity needs to be minimized for new applications and not unduly difficult for existing applications.

3. **Authentication Capabilities**—IAM/SSO infrastructure should support common user ID and password authentication and be extensible to

support multi factor authentications, such as tokens, biometrics, and smart cards.

4. **Shared Work Environments**—The IAM/SSO system must be able to authenticate across organizational boundaries and facilitate shared access to resources from disparate business units, or trusted external business partners.

5. **Overall Security Objectives**—The IAM/SSO infrastructure must provide audit capabilities for tracking who has access to applications and when that access was allowed. The infrastructure needs to be highly secure and redundant to minimize access disruption.

6. **User Access Management**—The IAM/SSO system must facilitate user access to network and application resources based upon roles and established rights. Users must be able to reset and manage their own passwords, and in the case of some classes of users, be able to add themselves to the directory component of the IAM.

7. **Single Sign-Off**—The IAM/SSO environment should support automated sign-off from applications once the user has logged out. This can be persistence based or a global sign-off once a user is no longer logged in to the network.

8. **Enterprise Reliability and Scalability**—The IAM/SSO environment must scale to meet high levels of demand and must be highly reliable (generally over five nines of reliability) to ensure uninterrupted access to resources.

9. **Legacy Application Integration**—The IAM/SSO system should be able to integrate with legacy authentication environments such as RACF and large specialized application directories to create a single access point for authentication, and access irrespective of the resource.

Emerging Technologies and Trends

Forrester[4] has identified leaders in this space and these are illustrated in Figure 4. In order to be included, the vendor had to meet the following requirements:

- A rich IAM portfolio. The vendor must own (not OEM or resell) IAM products in the core areas of provisioning, Web SSO, and federation.

- Established a depth of market penetration. The vendor must have IAM product revenues that exceed $25 million (excluding related implementation services).

[4] Cser, Andras, with Jonathan Penn, Paul Stamp, and Allison Herald, *The Forrester Wave™: Identity And Access Management, Q1 2008*, Forrester Research, March 14, 2008.

- Established a breadth of market penetration. The vendor must have more than one IAM product to which they can attribute $10 million in revenue or have $20 million in revenue attributable to an IAM suite.

It is important to note that neither Forrester nor Gartner make a concerted effort to compare open source IAM/SSO environments, such as OpenID. The results are clearly skewed toward substantial commercial vendor products and suites.

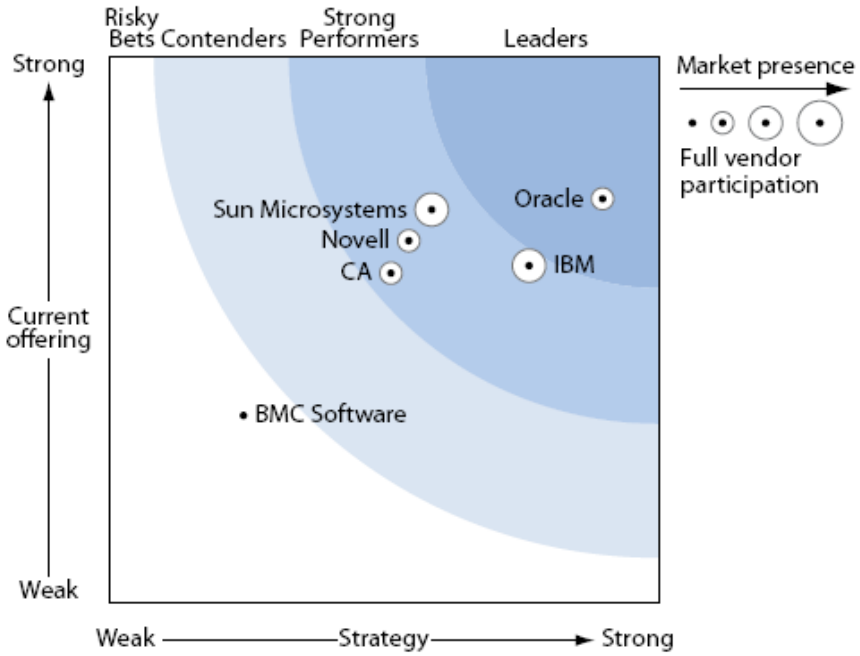

Figure 4. Forrester Wave ™ Identity Management Vendors

These criteria dramatically reduced the numbers of qualifying vendors. In summary, Forrester established the following observations:

- **Oracle has Established Itself as Leader**—Oracle has dedicated resources to building a versatile and well-rounded IAM product line. In addition to Oracle Identity Manager (OIM) and Oracle Access Manager (OAM), its recent acquisition and integration of role management and risk based authentication products help Oracle position its IAM product set as an identity services foundation.

- **Strong Performers**—IBM, Sun, Novell, and CA offer strong, competitive options. Each of these vendors has excellent product capabilities, a track record of delivering value to customers, and useful development plans. All of these vendors had areas that called for fundamental improvement.

Forrester observed that the IAM market of which SSO is a core component is on a trajectory for rapid growth. Federated identity is a topic of widespread interest,

but the level of interest outpaces the market's adoption of the technology. Federation's low adoption rate is indicative of process and technology issues including: difficulties in forming many-to-many trust relationships, incompatible protocols, and performance problems. Identity management has successfully thrived amid IT and business change because of its composite nature in both products and benefits.

Gartner released a Magic Quadrant report[5] on SSO in 2007. The Gartner Magic Quadrant for this IAM application component area is illustrated in Figure 5.

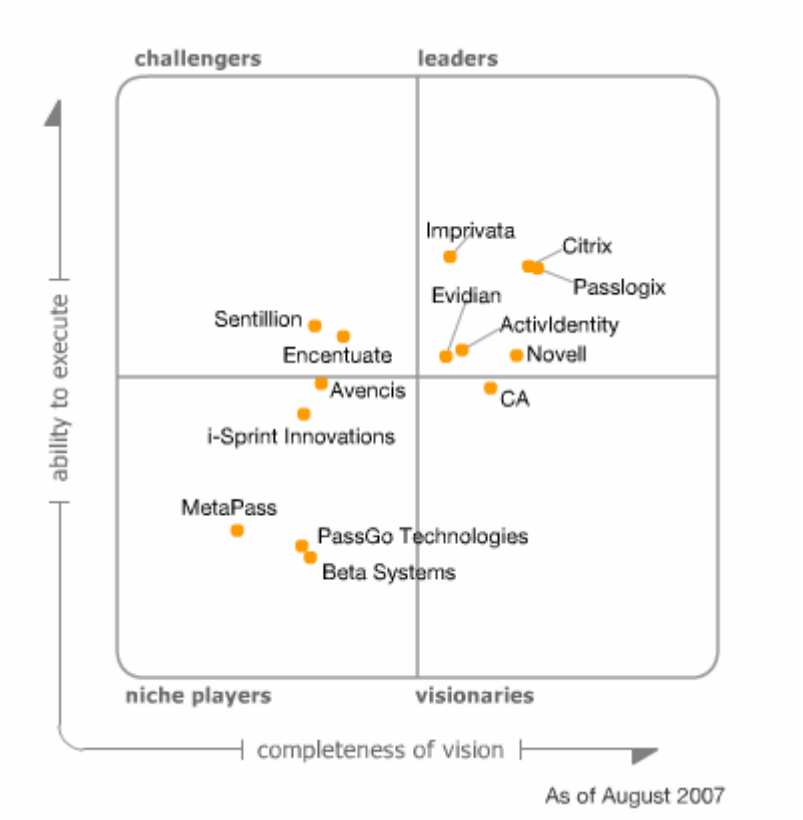

Figure 5. Magic Quadrant for Enterprise Single Sign-On, 2007

Gartner suggests[6] that "Improved user convenience and support cost reductions remain the top drivers for clients implementing enterprise single sign-on (ESSO). The 'sweet spots' for ESSO implementations are in enterprises where password-related help desk costs are high, shared-workstation support is needed, and users must manage a sustained, politically unacceptable number of user IDs and passwords."

[5] Kreizman, Gregg, *Magic Quadrant for Enterprise Single Sign-On, 2007*, Gartner RAS Core Research Note G00150863, August 30, 2007.
[6] *Ibid.*

Market competition has created downward-pricing pressures. Gartner[7] says that "Larger vendors with broad sales and integrator resources had significant growth in customers, although several small vendors' sales stagnated. ESSO tools are still imperfect in their abilities to integrate easily with all possible target systems using "out of the box" administrative tools. However, integration capabilities are improving across the board."

Open ID

OpenID[8] is a single sign-on system that allows Internet users to log on to different Web sites using a single digital identity, eliminating the need for a different user name and password for each site. An OpenID provider can be chosen by the user that best meets user needs and is deemed as a trusted provider. OpenID can stay with the user, no matter which provider is used or to which the user may migrate in the future. OpenID technology is not proprietary and represents no cost to the user. The OpenID architecture as it might be deployed by the State is illustrated[9] in Figure 6.

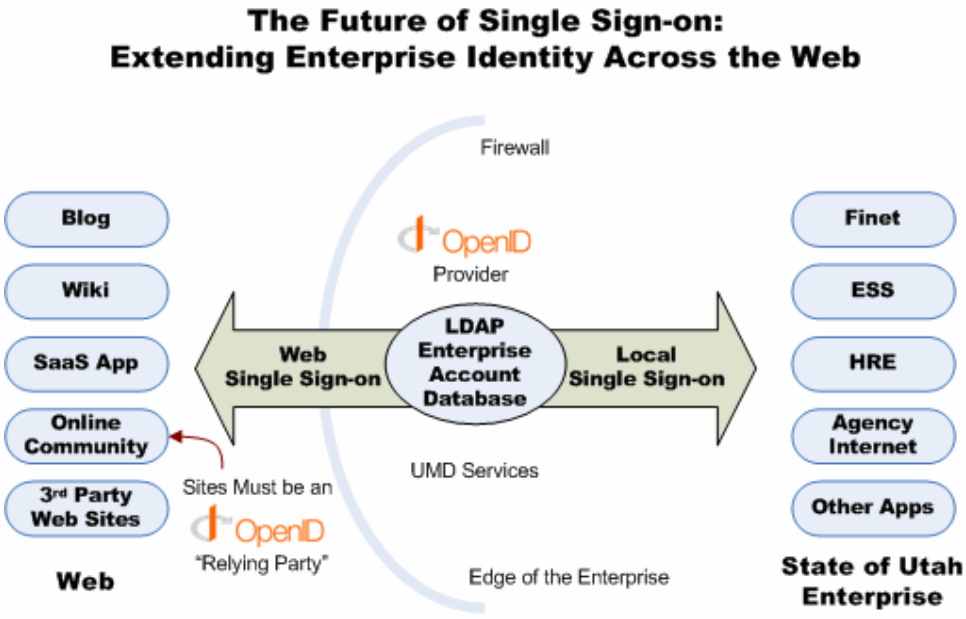

Figure 6. Extending Enterprise Identity across the Web

From a businesses perspective, this means a lower cost of password and account management, while potentially gaining new Web traffic. OpenID has been designed to lower user frustration by letting users have control of their login.

---

[7] *Ibid.*
[8] *What is OpenID?* at http://openid.net/what
[9] Hinchcliffe, Don, *openid: The once and future enterprise Single Sign-On?*, ZDNet Blog, February 4, 2008 at http://blogs.zdnet.com/Hinchcliffe

From a technical viewpoint OpenID is a decentralized, free framework for user-centric digital identity. OpenID takes advantage of already existing Internet technology (URI, HTTP, SSL, Diffie-Hellman) and realizes that people are already creating identities for themselves. With OpenID the user can easily transform one of these existing URIs into an account that can be used at sites which support OpenID logins.

OpenID is still in the early adoption phase, but it is becoming more popular, as large organizations like AOL, Google, Yahoo, Microsoft, Sun, Novell, etc. begin to accept and provide OpenIDs. It is estimated that there are over 160-million OpenID enabled URIs with nearly ten-thousand sites supporting OpenID logins. Open ID should be a consideration for the State's SSO infrastructure, especially for citizen use.

Federal Trends and Directions

Launched in 2002 as the E-Authentication Initiative, and as part of the President's Management Agenda, the E-Authentication Solution assists Federal agencies in meeting two primary goals[10]:

- **"**Mitigate the security and privacy risks associated with electronic government by allowing government agencies to develop trust relationships with their respective user communities through the use of electronic identity credentials (e.g., PKI certificates; user IDs/passwords) issued by other agencies and commercial organizations."

- **"**Control costs associated with authenticating the identity of a large number of end users by eliminating the need for each agency to create and maintain a separate credentialing system for each of their online applications."

The E-Authentication Solution created the US E-Authentication Identity Federation which allows Federation members to recognize and trust log-in IDs that are issued by other trusted Federation members. The trusted members that issue these log-in IDs may be other government agencies, academic institutions, or commercial entities, such as banks or other financial services institutions. There is opportunity for Utah to participate in this initiative by establishing the UMD as a trusted entity.

Through the US E-Authentication Identity Federation a citizen will be able to access government services using a login ID they already have from a Web site they trust, similar to the concept behind OpenID, rather than having to create another user ID and password.

[10] *E-Authentication: Secure Government Access Online*, at http://www.cio.gov/eauthentication

Financial Analysis

The overall UMD project costs[11] from initial implementation through June of 2007 were as follows:

Consulting	$ 320,000	Initial Software	$ 430,000
5yr Software maintenance	$ 280,000	Hardware	$ 120,000
5yr Hardware maintenance	$1,160,000	Personnel	$ 212,000
Total Cost		**$2,522,000**	

The NASCIO award application from which these costs were derived shows a substantial ROI benefit of close to 6:1 over the above costs. The reduction in help desk calls alone tends to at least partially justify the ROI numbers, especially if help desk calls are in the standard cost range of $30-50 per call.

Security Review and Analysis

The DTS Security Group needs to perform a specific audit of existing UMD security and document strengths and weaknesses so the product can be improved. Special emphasis is needed on the direct LDAP planned functionality and its impact on the UMD security model.

Operational and Infrastructure Analysis

From an operational perspective, Layer 4 needs immediate attention for UMD Services. The engineering design currently anticipates this implementation and it will have a positive impact on UMD Services availability, scalability, and reliability.

Solution Delivery Impact and Analysis

Solution delivery developers need to clearly articulate their requirements so UMD utilization is easier for them. Engineering staff working with UMD Services need to be highly responsive to documented needs from this user community. If this is not done, the developers will perpetuate the use of application specific directories and higher long term management costs.

Agency Services Impact and Analysis

The largest impact of UMD Services use in agencies is the long term elimination of costs currently charged for application directory management as a part of agency cost structures.

Summary and Recommendations

The UMD Services provided by the State constitute a highly secure and flexible IAM environment with capable SSO functionality. The services used from vendors such as Novell eDirectory and SiteMinder are highly regarded by

[11] *UMD: Utah Master Directory*, NASCIO Award Submittal, June 2007.

analysts and appear to form a useful foundation. In summary, the strengths of the existing UMD environment are as follows:

- UMD directory services are a highly scalable LDAP directory infrastructure.
- SiteMinder is one of the top rated access control Web SSO products.
- The Java applications for profile and application administration are capable and have in many cases more functionality than some commercial counterparts.
- The environment as designed and ultimately implemented with full Layer 4 support will be even more highly available and reliable than it is today.
- Ability to integrate multiple directory infrastructures including legacy environments such as RACF is strong but somewhat underutilized.
- Overall costs for operation and maintenance of the environment seem to be substantially lower than estimates by Forrester and Gartner.
- Time to benefit for implementing UMD Services within new applications is short compared to other competitive environments.
- User managed password functionality works well, as does the capability for external users to add themselves to the UMD directory as needed based upon application business requirements.
- The cost savings for UMD integration are well demonstrated with the low volume of help desk password and other UMD related calls.

The UMD Services offered by the State also have areas of weakness that should be addressed including:

- Easier to use identity management software. The existing software is very capable but lacks some of the user interface requirements found in many of its commercial counterparts.
- Documentation for developers is generally weak and needs to be substantially improved if adoption is to grow.
- Documentation for system administrators is needed so they can more effectively address UMD Services' integration and implementation issues.
- Documentation and benefits information for business entities is almost non-existent.
- Perceived difficulties with SiteMinder need to be addressed from a developer's perspective so they have a realistic expectation of capabilities and integration issues.
- Additional Web services are needed for .NET users, and providers for other application development environments supported by the State are needed.
- Lack of policy guidelines for utilizing the UMD in preference to application specific directory environments leave the UMD as a largely opt in environment.

- Lack of a policy and a well documented approach to use direct LDAP with the directory infrastructure.
- Lack of any explicit policy support requiring UMD use as a trusted identity on the DTS executive management level.

Recommendations
Based upon an overall assessment of the existing UMD Services, other alternatives used by agencies, and by Utah Interactive (UI) at the State portal site, the following are recommended actions:

- Position UMD Services as more than just a directory or SSO solution but as a comprehensive IAM solution.

- Establish the UMD as a trusted identity source so State users can use UMD identity to access Federal applications and services as a trusted partner.

- Add third party reporting software, such as eIQ, LogRhythm, etc., to facilitate audit tracking of who has access to directory enabled resources, and when they had access.

- Improve the user interface for AppAdmin and AppProfile so they are easier to use by the development and application business management communities.

- Meet with members of the development community to better understand their needs for UMD Services and their specific requirements.

- Provide effective documentation of UMD Services for the developer community.

- Provide capability for direct LDAP access by agencies within security model constraints.

- Appoint a study group to review UI authentication and look at possible integration of their 36,857 directory subscribers with the UMD directory as a specialized container.

- Review other State directory pools for inclusion in the UMD (e.g. Drivers License, Voter Registration, eREP, etc.)

- Review possible integration of UMD Services with OpenID, especially for citizen users, and establish the State as an OpenID provider.

- Establish a formal DTS policy that requires UMD use for new application development and establishes it as a trusted identity source.

- Require agencies to log Help Desk calls for applications that do not use UMD Services to better assess true costs of application specific directory management.

- Establish ongoing training for UMD Services at the Agency IT management, business and developer level with appropriate supporting collateral and Web resources.

- Measure and report the cost benefits of UMD Services use.

- Assess the burdened costs to DTS for application specific directory implementations in agencies.

- Document and promote the security advantages from utilizing UMD Services.

UMD Services, as they exist today, are substantially ahead of most States and offer features and functions not commonly found in any but the most expensive commercial applications. Only about one third of the SSO survey audience perceived a clear need for application directory integration and SSO. This strongly suggests the need for training and documentation. Changing technologies at this point will have minimal impact.

References

Cicchitto, Nelson, *Evaluating Your Identity and Access Management Options*, IT Security Journal, October 1, 2007.

Cser, Andras, with Jonathan Penn, Paul Stamp, and Allison Herald, *The Forrester Wave™: Identity And Access Management, Q1 2008*, Forrester Research, March 14, 2008.

_____, and Penn, Jonathan, *Identity Management Market Forecast: 2007 To 2014*, Forrester Research, February 2008.

_____, with Jonathan Penn and Allison Herald,The State Of Federation, Forrester Research, September 27, 2007.

E-Authentication: Secure Government Access Online, at http://www.cio.gov/eauthentication

Hinchcliffe, Don, *openid: The once and future enterprise Single Sign-On?*, ZDNet Blog, February 4, 2008 at http://blogs.zdnet.com/Hinchcliffe

Kreizman, Gregg, *Magic Quadrant for Enterprise Single Sign-On, 2007*, Gartner RAS Core Research Note G00150863, August 30, 2007.

Liou, Michael, *Enterprise Single Sign-On Best Practice Considerations*, Computer Associates: Identity and Access Management, August 2007.

Rubio, Daniel, *OpenID: Leveraging a widely accepted identity Web service*, SearchSOA.com, March 18, 2008, at http://searchsoa.techtarget.com/tip/0,289483,sid26_gci1305991,00.html?track=NL-449&ad=630060&asrc=EM_NLT_3289956&uid=6075716#

Penn, Jonathan, *Justifying E-SSO: Benefits Beyond the Help Desk,* Forrester Research, July 6, 2006.

_____*, Single Sign-On: Dispelling the Myths, Finding the Fit,* Forrester Research, 2006.

_____, with Bruce D. Temkin and Adele Sage, *Strong Authentication And Enterprise Single Sign-On Go Hand In Hand*, Forrester Research, September 21, 2005.

Phifer, Lisa, “Identity management appliances reduce password cost.” Core Competence, July 21, 2006.

UMD: Utah Master Directory, NASCIO Award Submittal, June 2007.

Utah Master Directory Operational Overview, State of Utah: NUI, September 24, 2002 at http://nui.state.ut.us/technotes/UMD_Operational_Overview.htm

Wayment, Dawn, *Password and UMD Help Desk Statistics*, Department of Technology Services, March 17, 2008.

What is OpenID? at http://openid.net/what

APPENDIX A. SSO SURVEY RESPONSE SUMMARY

1. What methods are currently used in your agency for Web-based authentication, authorization, and Single-Sign-On (SSO)?

Utah Master Directory/SiteMinder:	65.4%	17
Application Specific Directory and Authorization:	65.4%	17
Direct LDAP to Agency Directory Information:	23.1%	6
Agency SSO:	3.8%	1
Other (please specify):		
No Method:	11.5%	3
Active Directory to UMD Sync:	3.8%	1
N = 28		
Answered Question:	26	(92.9%)
No Response:	2	(7.1%)

2. Approximately how many Web applications requiring authentication are deployed by your agency?

Specify approximate number of applications:	248	
What % is only for internal use by agency employees?:	72.7 %	
What % is for public and/or external use?:	68.2 %	
What % is for other use or not applicable?:	5.24 %	
N = 28		
Answered Question:	22	(78.6%)
No Response:	6	(21.4%)

3. Of the methods selected above, what is the approximate frequency for each option as a percentage of all of your Web applications?

Utah Master Directory/SiteMinder:	36.4%	
Application Specific Directory and Authorization:	72.7%	
Direct LDAP to Agency Directory Information:	31.8%	
Agency SSO:	9.1%	
Other:	9.1%	
N = 28		
Answered Question:	22	(78.6%)
No Response:	6	(21.4%)

4. If you are currently using the UMD/SiteMinder infrastructure, what are the features that are working best for your agency?

Integration with NDS to Synchronize LAN Passwords:	50.0%	11
Availability of UMD/SiteMinder Infrastructure:	40.9%	9
Identity Management:	22.7%	5
Simplified Maintenance of User Access Privileges:	18.2%	4
UMD Support Services:	18.2%	4
Reliability and Scalability:	4.5%	1
Developer Documentation:	0.0%	0
Other (Not Using UMD/SiteMinder):	40.9%	9
N = 28		
Answered Question:	22	(78.6%)
No Response:	6	(21.4%)

5. If you are currently using the UMD/SiteMinder infrastructure, what are the features that are not working to your satisfaction for your agency?

Not Applicable:	45.5%	10
SiteMinder:	13.6%	3
Works as described—No Issues:	13.6%	3
UMD Synchronization:	9.1%	2
Configuration and Setup:	9.1%	2
Regulatory Compliance:	4.5%	1
Support:	4.5%	1
N = 28		
Answered Question:	22	(78.6%)
No Response:	6	(21.4%)

6. What are the obstacles that keep your agency from using enterprise directory resources such as the UMD/SiteMinder?

Difficulty Using the UMD with New Applications:	22.7%	5
Difficulty Using the UMD with Existing Applications:	22.7%	5
Direct LDAP Access:	18.2%	4
Reliability and Scalability Concerns:	18.2%	4
Inadequate Documentation:	13.6%	3
Cost Concerns:	13.6%	3
Availability of UMD Web Services:	13.6%	3
Application Profile Management:	9.1%	2
SSO Security Concerns:	9.1%	2
Concerns with the Use of “Cookies”:	4.5%	1
Other:		
Adding and Managing External Users:	13.6%	3
Duplication of Existing Application Authentication:	9.1%	2
No Known Obstacles:	9.1%	2

Not Applicable:	9.1%	2
Never Looked Into Using UMD/SiteMinder:	9.1%	2
Performance:	. 5%	1
N = 28		
Answered Question:	22	(78.6%)
No Response:	6	(21.4%)

7. Does your agency perceive a need for SSO functionality across its Web-based applications? Please indicate the priority and importance your agency places on SSO (5 Highest–1 Lowest) importance.

5—Highest Priority:	9.1%	2
4—High Priority:	27.3%	6
3—Moderate Priority:	18.2%	4
2—Low Priority:	4.5%	1
1—Lowest Priority:	40.9%	9
N = 28		
Answered Question:	22	(78.6%)
No Response:	6	(21.4%)

8. How important is directory integration with enterprise SSO capability for legacy, anything that isn't Web-based (e.g., mainframe, client server, etc.), for your agency (5 Highest–1 Lowest) importance.

5—Highest Priority:	18.2%	4
4—High Priority:	9.1%	2
3—Moderate Priority:	9.1%	2
2—Low Priority:	22.7%	5
1—Lowest Priority:	40.9%	9
N = 28		
Answered Question:	22	(78.6%)
No Response:	6	(21.4%)

9. Does your agency have a need for strong authentication capabilities (e.g., multi-factor beyond just login/password) within an enterprise SSO service offering? Please indicate the priority and importance that your agency places on strong authentication (5 Highest–1 Lowest) importance.

5—Highest Priority:	22.7%	5
4—High Priority:	9.1%	2
3—Moderate Priority:	13.6%	3
2—Low Priority:	13.6%	3
1—Lowest Priority:	22.7%	5
Not Applicable:	18.2%	4
N = 28		
Answered Question:	22	(78.6%)
No Response:	6	(21.4%)